Understanding Localized-Scanning Worms

Zesheng Chen
School of Electrical &
Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332
Email: zchen@ece.gatech.edu

Chao Chen
Department of Engineering
Indiana University - Purdue
University Fort Wayne
Fort Wayne, IN 46805
Email: chen@engr.ipfw.edu

Chuanyi Ji
School of Electrical &
Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332
Email: jic@ece.gatech.edu

Abstract— **Localized scanning is a simple technique used by attackers to search for vulnerable hosts. Localized scanning trades off between the local and the global search of vulnerable hosts and has been used by Code Red II and Nimda worms. As such a strategy is so simple yet effective in attacking the Internet, it is important that defenders understand the spreading ability and behaviors of localized-scanning worms. In this work, we first characterize the relationships between vulnerable-host distributions and the spread of localized-scanning worms through mathematical modeling and analysis, and compare random scanning with localized scanning. We then design an optimal localized-scanning strategy, which provides an upper bound on the spreading speed of localized-scanning self-propagating codes. Furthermore, we construct three variants of localized scanning. Specifically, the feedback localized scanning and the ping-pong localized scanning adapt the scanning methods based on the feedback from the probed host, and thus spread faster than the original localized scanning and meanwhile have a smaller variance.**

I. Introduction

Self-propagating Internet worms have posed significant threats to network security. For example, Code Red [7], Nimda [20], and Witty [10] worms infected hundreds of thousands of computers and cost tremendous efforts to eliminate them. Therefore, it is important that we understand how worms spread to design effective countermeasures accordingly.

A worm spreads by using distinct scanning mechanisms including topological and hitlist scanning [12]. Our focus, however, is only on scanning worms that probe the entire IPv4 address space or the routable address space, such as random, routable, importance, and localized scanning. *Random scanning* chooses target IP addresses at random and is exploited by Code Red and Witty worms. *Routable scanning* selects targets only in the routable address space by using the information provided by BGP routing table [14], [16]. *Importance scanning* exploits an uneven distribution of vulnerable hosts and focuses worm scans on the most relevant parts of the IPv4 address space [4], [3].

In this work, our focus is on localized scanning, which has been used by such famous worms as Code Red II and Nimda. *Localized scanning* preferentially searches for vulnerable hosts in the "local" address space. For example, the Code Red II worm selects target IP addresses as follows [19]:

- 50% of the time, an address with the same first byte is chosen as the target,
- 37.5% of the time, an address with the same first two bytes is chosen as the target,
- 12.5% of the time, a random address is chosen.

Song et al. showed that Nimda and Code Red II worms accounted for 90% infection attempts in the seven-week period from September 19 to November 3, 2001 [11]. Why is such a localized strategy so effective? It has been observed that in the current Internet, a sub-network intends to have many computers with the same operating systems and applications for easy management [9]. Hence, vulnerable hosts usually form clusters [2]. Once a vulnerable host in such a subnet is infected, a localized-scanning worm can rapidly compromise all the other local vulnerable hosts.

The goal of this work is to better understand the spreading ability and characteristics of localized-scanning worms. Specifically, we attempt to answer the following questions:

- What is the effect of vulnerable-host distributions on the spread of localized-scanning worms? The prior work has studied this effect empirically [2], [17], [9]. In this work, we use mathematical reasoning to show the relationships between vulnerable-host distributions and localized-scanning worms. Specifically, it is shown analytically that localized-scanning worms spread slower than random-scanning worms if vulnerable hosts are uniformly distributed, or faster if highly unevenly distributed. Moreover, if infected hosts are uniformly distributed, localized-scanning worms can speed up the propagation with nearly a rate of the non-uniformity factor that quantifies the non-uniformity of a vulnerable-host distribution [5].
- What is the propagation capacity of a localized-scanning worm? We design an optimal localized-scanning strategy that maximizes the localized-scanning worm propagation speed. Such a strategy dynamically adapts the parameters used for scanning the local sub-network and the global Internet, based on the distribution of uninfected vulnerable hosts. Although the optimal localized scanning is difficult to implement, it provides an upper bound on the spreading speeds of the currently used localized scanning and its variants. Moreover, we empirically show that the propagation speed of the currently used localized scanning can approach that of the optimal strategy.
- What are some possible variants of localized-scanning worms? We study three variants of localized scanning

that can be easily implemented. The first one makes an infected host focus on scanning either locally or globally. Such a variant, however, is shown empirically to spread slower and have a larger variance than localized scanning. Therefore, it may not be a good candidate for worm attacks. The second variant is inspired by the optimal localized scanning. Specifically, an infected host initiates to scan the local sub-network and switches to scanning the global Internet when it probes a local host that has been already infected. Such a strategy makes an infected host adapt scanning strategies dynamically, based on the feedback from the probed host. We show that this simple variant can spread faster than localized scanning and has a smaller variance. Therefore, this scanning method is a potential tool for attackers. The second variant is easily extended to a "ping-pong" algorithm, which further improves the worm spreading speed at the late stage.

The remainder of this paper is structured as follows. Section II provides the background on localized scanning and vulnerable-host distributions. Section III shows the effect of vulnerable-host distributions on localized scanning analytically. Sections IV and V design the optimum and the variants of localized scanning. Section VI concludes the paper.

II. Preliminaries

A. *Localized Scanning*

Localized scanning preferentially scans for targets in the address space that is close to the victim. The basic idea of such a scanning method is that if vulnerable hosts are clustered, an infected host searching for local hosts would have a higher probability to find a target than random guessing. Localized scanning has been exploited by Code Red II and Nimda worms [19], [20]. Moreover, the Blaster worm also uses localized scanning to select its starting point [21]. The successes of these worms indicate the effectiveness of such a simple scanning strategy.

In this work, we consider two types of localized scanning (LS). The first type is a simplified version of LS, called */l LS*, which scans the Internet as follows:

- p_a $(0 \leq p_a \leq 1)$ of the time, an address with the same first l bits is chosen as the target,
- $1 - p_a$ of the time, a random address is chosen.

When $p_a = 0$, /l LS is identical to random scanning (RS). Here, we use the classless inter-domain routing (CIDR) notation. The IPv4 address space is partitioned into subnets according to the first l bits of IP addresses, i.e., /l prefixes or /l subnets, where $l \in \{0, 1, , \cdots, 32\}$. Thus, each /$l$ subnet i $(i = 1, 2, \cdots, 2^l)$ has 2^{32-l} addresses.

The second type is called *two-level LS* (2LLS), which has been used by the Code Red II and Nimda worms. 2LLS scans the Internet as follows:

- p_b $(0 \leq p_b \leq 1)$ of the time, an address with the same first byte is chosen as the target,
- p_c $(0 \leq p_c \leq 1 - p_b)$ of the time, an address with the same first two bytes is chosen as the target,
- $1 - p_b - p_c$ of the time, a random address is chosen.

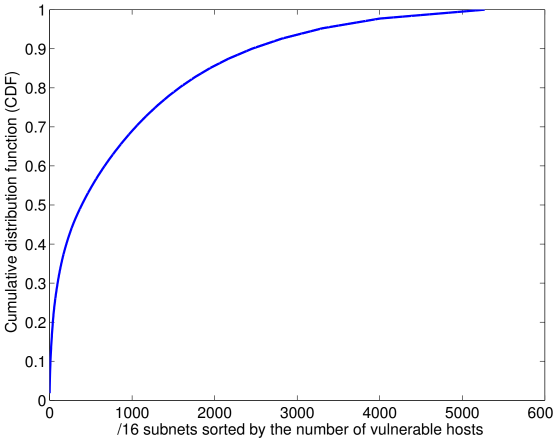


Fig. 1. CDF of the percentage of Witty-worm victims in sorted /16 subnets.

For example, for the Code Red II worm, $p_b = 0.5$ and $p_c = 0.375$ [19]; for the Nimda worm, $p_b = 0.25$ and $p_c = 0.5$ [20].

Only a handful work has been carried out on localized scanning. Chen et al. pointed out that if the vulnerable hosts are uniformly distributed in the IPv4 address space, localized scanning spreads at a slightly slower rate than random scanning [2]. Zou et al. showed that if the vulnerable hosts are uniformly distributed only in the routable address space, localized scanning has a spreading speed comparable to Class-A routable scanning [17]. Rajab et al. further demonstrated that if the vulnerable hosts follow a power law distribution, localized scanning can propagate much faster than random scanning [9]. The prior work, however, focuses on simulation comparisons between localized scanning and random scanning. The mathematical reasoning on these comparisons has not been studied.

B. *Vulnerable-Host Distribution*

The prerequisite for localized scanning is that vulnerable hosts are non-uniformly distributed in the Internet. The non-uniformity of vulnerable-host distributions has been observed in prior work [1], [7], [8], [10], [9], [4]. Taking the distribution of Witty-worm victims among /16 subnets as an example, we process the data provided by CAIDA [18] as follows. First, the /16 subnets are sorted decreasingly according to the number of vulnerable hosts. Then, the empirical cumulative distribution function (CDF) of the percentage of vulnerable hosts in the sorted /16 subnets is computed and plotted in Figure 1. We find that 1,573 (2.4%) /16 subnets contain 80% vulnerable hosts, whereas 2,453 (3.7%) /16 subnets hold 90% vulnerable hosts. Therefore, only a small percentage of /16 subnets contain a large portion of vulnerable hosts, and the distribution of Witty-worm victims is highly non-uniform.

C. *Non-Uniformity Factor*

How can we quantify the non-uniformity of a vulnerable-host distribution? In our prior work [5], we use a simple metric, called the *non-uniformity factor*, to measure the non-uniformity of a distribution.

Let N be the total number of vulnerable hosts and $N_i^{(l)}$ be the number of vulnerable hosts in /l subnet i ($i = 1, 2, \cdots, 2^l$). Define $p_g^{(l)}(i) = \frac{N_i^{(l)}}{N}$, which is called the group distribution in /l subnets. Then, the non-uniformity factor in /l subnets is defined as

$$\beta^{(l)} = 2^l \sum_{i=1}^{2^l} \left(p_g^{(l)}(i)\right)^2. \tag{1}$$

A larger non-uniformity factor indicates a more non-uniform distribution. When a vulnerable-host distribution is uniform among /l subnets, $\beta^{(l)} = 1$. For the Witty-worm victim distribution, $\beta^{(8)} = 12.0$ and $\beta^{(16)} = 126.7$.

III. Effect of Vulnerable-Host Distributions on Localized Scanning

In this section, we study the effect of vulnerable-host distributions on localized scanning and compare the spreading dynamics of localized-scanning (LS) worms with those of random-scanning (RS) worms by modeling their propagation. As a dynamic worm-propagation model is non-linear, it is difficult to result in a close-form solution. Hence, we gain some insights through exploring extreme cases of vulnerable-host and infected-host distributions among subnets. Specifically, we consider three extreme cases: (1) Vulnerable hosts are evenly distributed, (2) Vulnerable hosts are highly unevenly distributed, and (3) Infected hosts are uniformly distributed.

A simple abstract model, known as the *susceptible → infected* (SI) model, has been exploited to model the spread of worms in various earlier work [12], [16]. The SI model assumes that each host has two states: susceptible and infected. Once infected, a host stays in the infected state. Here, we adopt a discrete-time SI model. In particular, we employ the analytical active worm propagation (AAWP) model, which was proposed by Chen et al. in [2] and has been applied in [9], [6], [14].

A. Random Scanning

In the AAWP model, the spread of RS worms is characterized as follows [4]:

$$\begin{aligned} I_{t+1} &= I_t + (N - I_t)\left[1 - \left(1 - \frac{1}{\Omega}\right)^{I_t s}\right] \qquad (2) \\ &= I_t + (N - I_t)\frac{I_t s}{\Omega} - O\left(\frac{1}{\Omega^2}\right), \qquad (3) \end{aligned}$$

where I_t is the average number of infected hosts at time t ($t \geq 0$); N is the total number of vulnerable hosts; s is the scanning rate; and Ω is the scanning space. Since $\Omega = 2^{32} >> 1$, we ignore $O\left(\frac{1}{\Omega^2}\right)$ and have

$$I_{t+1} = I_t + \frac{(N - I_t)I_t s}{\Omega}. \tag{4}$$

B. /l Localized Scanning

The AAWP model can be extended to model the spread of /l LS worms:

$$\begin{aligned} I_{t+1,i}^{(l)} &= I_{t,i}^{(l)} + (N_i^{(l)} - I_{t,i}^{(l)})\left[1 - \left(1 - \frac{1}{\Omega_i}\right)^{S_{t,i}}\right] \qquad (5) \\ &= I_{t,i}^{(l)} + (N_i^{(l)} - I_{t,i}^{(l)})\frac{S_{t,i}}{\Omega_i} - O\left(\frac{1}{\Omega_i^2}\right), \qquad (6) \end{aligned}$$

where $i = 1, 2, \cdots, 2^l$; $I_{t,i}^{(l)}$ is the expected number of infected hosts in /l subnet i at time t ($t \geq 0$); $N_i^{(l)}$ is the number of vulnerable hosts in /l subnet i; Ω_i is the size of the address space in /l subnet i; and $S_{t,i}$ is the average number of scans hitting /l subnet i during time period $(t, t+1]$. Since $\Omega_i = 2^{32-l} >> 1$, we ignore $O\left(\frac{1}{\Omega_i^2}\right)$. Summing over $i = 1, 2, \cdots, 2^l$ on both sides of Equation (6), we have

$$I_{t+1} = I_t + \sum_{i=1}^{2^l} \frac{\left(N_i^{(l)} - I_{t,i}^{(l)}\right) S_{t,i}}{2^{32-l}}, \tag{7}$$

where $I_t = \sum_{i=1}^{2^l} I_{t,i}^{(l)}$.

The average number of scans that fall into /l subnet i during the time period $(t, t+1]$ (i.e., $S_{t,i}$) consists of two parts: (a) $p_a I_{t,i}^{(l)} s$ scans from local infected hosts within subnet i and (b) $\frac{(1-p_a)I_t s}{2^l}$ scans from all infected hosts. That is,

$$S_{t,i} = \left(p_a I_{t,i}^{(l)} + \frac{1 - p_a}{2^l} I_t\right) s, \qquad i = 1, 2, \cdots, 2^l. \tag{8}$$

Putting Equation (8) into Equation (7), we have

$$\begin{aligned} I_{t+1} &= I_t + (1 - p_a)\frac{(N - I_t)I_t s}{\Omega} \\ &\quad + p_a \frac{s}{\Omega} \cdot 2^l \sum_{i=1}^{2^l} \left(N_i^{(l)} - I_{t,i}^{(l)}\right) I_{t,i}^{(l)}. \qquad (9) \end{aligned}$$

On the right-hand side of the above equation, the second term represents the random-scanning component in the /l LS, while the third term corresponds to the preference of scanning the local /l subnet. If $\frac{(N-I_t)I_t s}{\Omega} \leq \frac{s}{\Omega} \cdot 2^l \sum_{i=1}^{2^l} \left(N_i^{(l)} - I_{t,i}^{(l)}\right) I_{t,i}^{(l)}$, a /$l$ LS worm should choose a large value of p_a to speed up the propagation.

As a close-form expression for I_t is difficult to obtain, we consider three extreme cases of vulnerable-host and infected-host distributions. The first case assumes that vulnerable hosts are uniformly distributed, i.e., $N_1^{(l)} = N_2^{(l)} = \cdots = N_{2^l}^{(l)}$. Then, when $I_{t,i}^{(l)} > I_{t,j}^{(l)}$, $N_i^{(l)} - I_{t,i}^{(l)} < N_j^{(l)} - I_{t,j}^{(l)}$, $i, j \in \{1, 2, \cdots, 2^l\}$. This results in

$$\begin{aligned} & 2^l \sum_{i=1}^{2^l} \left(N_i^{(l)} - I_{t,i}^{(l)}\right) I_{t,i}^{(l)} \\ & < \left[\sum_{i=1}^{2^l} \left(N_i^{(l)} - I_{t,i}^{(l)}\right)\right] \left(\sum_{i=1}^{2^l} I_{t,i}^{(l)}\right) = (N - I_t)I_t, \qquad (10) \end{aligned}$$

assuming that the numbers of infected hosts among subnets are not all equal. The above relation is obtained by the Chebyshev sum inequality [13] or the rearrangement inequality [22]. The details of these two inequalities are given in the Appendix. When applying the result of Equation (10) to Equation (9), we obtain that $I_{t+1} < I_t + \frac{(N-I_t)I_t s}{\Omega}$. Therefore, the uniform distribution of vulnerable hosts leads to a low value of p_a for an effective /l LS worm. Moreover, the spread of /l LS worms is slower than that of RS worms in this case.

The second case assumes that vulnerable hosts are highly unevenly distributed so that when a /l subnet has more infected hosts, it would also contain more uninfected vulnerable hosts. That is, when $I_{t,i}^{(l)} > I_{t,j}^{(l)}$, $N_i^{(l)} - I_{t,i}^{(l)} > N_j^{(l)} - I_{t,j}^{(l)}$, $i, j \in \{1, 2, \cdots, 2^l\}$. We can then derive

$$2^l \sum_{i=1}^{2^l} \left(N_i^{(l)} - I_{t,i}^{(l)} \right) I_{t,i}^{(l)} > (N - I_t) I_t, \qquad (11)$$

assuming that the numbers of infected hosts among subnets are not all equal. The above relation is obtained by the Chebyshev sum inequality. When applying the result of Equation (11) to Equation (9), we obtain that $I_{t+1} > I_t + \frac{(N-I_t)I_t s}{\Omega}$. Therefore, for such an extreme case, a large value of p_a is preferred for an effective /l LS worm. Moreover, the spread of /l LS worms is faster than that of RS worms.

The last case assumes a uniform distribution of infected hosts among subnets. That is, the number of infected hosts in /l subnet i is proportional to the number of vulnerable hosts in this subnet, i.e., $I_{t,i}^{(l)} = I_t \cdot p_g^{(l)}(i)$, $i = 1, 2, \cdots, 2^l$. This assumption changes Equation (9) to

$$I_{t+1} = I_t + \left(1 - p_a + p_a \beta^{(l)} \right) \frac{(N - I_t) I_t s}{\Omega}, \qquad (12)$$

where $\beta^{(l)}$ is the non-uniformity factor as defined in Equation (1). Thus, compared with RS (Equation (4)), /l LS can increase the propagation speed with a rate of $1 - p_a + p_a \beta^{(l)}$. For example, when $p_a = 0.75$, a /8 LS Witty worm can increase the spreading speed with a factor of 9.25, whereas a /16 LS Witty worm can increase the speed with a factor of 95.28.

C. Two-Level Localized Scanning

For 2LLS, Equation (7) still holds when $l = 16$. The average number of scans hitting /16 subnet i during time period $(t, t+1]$ is

$$S_{t,i} = \left(p_c I_{t,i}^{(16)} + \frac{p_b}{2^8} \sum_{j \in A_i^{(8)}} I_{t,j}^{(16)} + \frac{1 - p_b - p_c}{2^{16}} I_t \right) s, \qquad (13)$$

where $i = 1, 2, \cdots, 2^{16}$; $A_i^{(8)}$ denotes the set of /16 subnets that have the same first byte of the subnet address as /16 subnet i; and $\sum_{j \in A_i^{(8)}} I_{t,j}^{(16)}$ represents the expected number of the infected hosts in the Class-A subnet that has the same first byte of the address as the /16 subnet i. Putting Equation (13) into Equation (7) and setting $l = 16$, we have,

$$\begin{aligned} I_{t+1} &= I_t + (1 - p_b - p_c) \frac{(N - I_t) I_t s}{\Omega} \\ &\quad + \frac{2^8 p_b s}{\Omega} \sum_{i=1}^{2^8} \left(N_i^{(8)} - I_{t,i}^{(8)} \right) I_{t,i}^{(8)} \\ &\quad + \frac{2^{16} p_c s}{\Omega} \sum_{i=1}^{2^{16}} \left(N_i^{(16)} - I_{t,i}^{(16)} \right) I_{t,i}^{(16)}. \qquad (14) \end{aligned}$$

Similar to /l LS, 2LLS can be shown to spread slower (or faster) than RS if vulnerable hosts are uniformly (or highly unevenly) distributed[1]. Moreover, if infected hosts are uniformly distributed, the model for the 2LLS (i.e., Equation (14)) becomes

$$\begin{aligned} I_{t+1} &= I_t + \left(1 - p_b - p_c + p_b \beta^{(8)} + p_c \beta^{(16)} \right) \cdot \\ &\quad \frac{(N - I_t) I_t s}{\Omega}. \qquad (15) \end{aligned}$$

Comparing Equations (4) with (15), we find that when p_c is large and the uniformity condition of infected hosts holds, a 2LLS worm can speed up the propagation nearly $\beta^{(16)}$ times compared with an RS worm.

Our findings provide quantifications to some of the previous observations [2], [17], [9]. For example, when vulnerable hosts are uniformly distributed, an LS worm propagates slower than an RS worm [2]. On the other hand, when the underlying vulnerable-host distribution follows nearly a power law, an LS worm can spread much faster than an RS worm [9].

IV. Optimal Dynamic Localized Scanning

What is the "best-case scenario" for LS worms? How different is the currently used LS from the optimal LS? To answer these questions, we study the optimal LS, focusing on /l LS for simplicity. The essential of the optimal LS is to choose the best parameters (i.e., p_a, p_b, and p_c) to maximize the propagation speed. Intuitively, the optimal LS should be dynamic and adjust its parameters during the scanning process. Hence, these parameters depend on the location of infected hosts and vary with time. We use $p_{t,i}^{(a)}$ to denote p_a at time t for an infected host in /l subnet i.

A. Optimal /l Localized Scanning

The optimal /l LS should determine $p_{t,i}^{(a)}$ $(0 \le p_{t,i}^{(a)} \le 1)$ to maximize the probability of finding an uninfected vulnerable host. To obtain this, we assume that the number of vulnerable hosts and the number of infected hosts in each subnet at time t (i.e., $N_i^{(l)}$'s and $I_{t,i}^{(l)}$'s) are known to the worm. Therefore, our problem reduces to obtaining the optimal $p_{t,i}^{(a)}$'s for worm propagation, given $N_i^{(l)}$'s and $I_{t,i}^{(l)}$'s.

For the dynamic /l LS, the average number of scans that fall into /l subnet i during time period $(t, t+1]$ (i.e., $S_{t,i}$) consists of two parts: (a) $p_{t,i}^{(a)} I_{t,i}^{(l)} s$ scans from local infected

[1] We omit the details of derivation for brevity.

TABLE I

SUMMARY OF THE OPTIMAL 2LLS.

Comparison	Result	Scanning strategy	Meaning
$\max\{N_i^{(16)} - I_{t,i}^{(16)},$ $\frac{1}{2^8}\sum_{j\in A_i^{(8)}}(N_j^{(16)} - I_{t,j}^{(16)}),$ $\frac{1}{2^{16}}(N - I_t)\}$	$N_i^{(16)} - I_{t,i}^{(16)}$	$p_{t,i}^{(b)} = 0$ and $p_{t,i}^{(c)} = 1$	scan only the local /16 subnet
	$\frac{1}{2^8}\sum_{j\in A_i^{(8)}}(N_j^{(16)} - I_{t,j}^{(16)})$	$p_{t,i}^{(b)} = 1$ and $p_{t,i}^{(c)} = 0$	scan only the local /8 subnet
	$\frac{1}{2^{16}}(N - I_t)$	$p_{t,i}^{(b)} = p_{t,i}^{(c)} = 0$	scan the global Internet randomly

hosts within subnet i and (b) $\frac{1}{2^l}\sum_{j=1}^{2^l}(1-p_{t,j}^{(a)})I_{t,j}^{(l)}s$ scans from all infected hosts. That is,

$$S_{t,i} = \left[p_{t,i}^{(a)} I_{t,i}^{(l)} + \frac{\sum_{j=1}^{2^l}(1-p_{t,j}^{(a)})I_{t,j}^{(l)}}{2^l}\right]s, \qquad (16)$$

where $i = 1, 2, \cdots, 2^l$. Putting Equation (16) into Equation (7), we have

$$\begin{aligned} I_{t+1} &= I_t + \frac{s}{2^{32-l}}\sum_{i=1}^{2^l} I_{t,i}^{(l)} \cdot \\ &\quad \left[p_{t,i}^{(a)}(N_i^{(l)} - I_{t,i}^{(l)}) + (1-p_{t,i}^{(a)})\frac{N-I_t}{2^l}\right]. \qquad (17) \end{aligned}$$

To maximize I_{t+1}, $p_{t,i}^{(a)}$ needs to satisfy

$$p_{t,i}^{(a)} = \begin{cases} 1, & \text{if } N_i^{(l)} - I_{t,i}^{(l)} > \frac{N-I_t}{2^l}; \\ 0, & \text{otherwise.} \end{cases} \qquad (18)$$

That is, if the number of uninfected vulnerable hosts in subnet i is larger than the average number of uninfected vulnerable hosts among 2^l subnets at time t, the infected hosts in sunbet i should scan only the local subnet; otherwise, the infected hosts should use random scanning. Thus, the propagation model for the optimal dynamic /l LS is

$$I_{t+1} = I_t + \frac{s}{2^{32-l}}\sum_{i=1}^{2^l} I_{t,i}^{(l)} \max\left\{N_i^{(l)} - I_{t,i}^{(l)}, \frac{N-I_t}{2^l}\right\}. \quad (19)$$

Using this optimal scanning method, a worm starting from a subnet that contains many vulnerable hosts would first scan locally. The infected hosts in this subnet then switch from scanning locally to scanning globally later when few uninfected vulnerable hosts remain. The key is that the worm switches the scanning strategy when it is aware of the change of the distribution of uninfected vulnerable hosts.

It should be noted that implementing such optimal LS is difficult. First, $N_i^{(l)}$'s may not be known in advance. Second, to perform this LS, each infected host needs to know $I_{t,i}^{(l)}$'s, which leads to numerous information exchanges among infected hosts. The optimal dynamic LS, however, provides the best scenario of LS and can be used as the baseline for designing some realistic LS worms.

B. Optimal Two-Level Localized Scanning

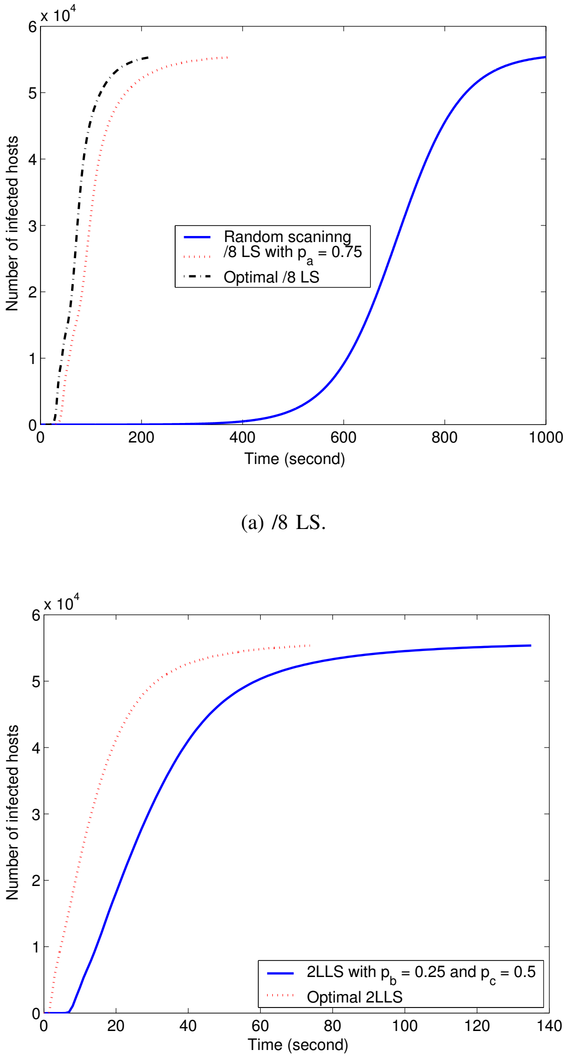
We can easily extend the above derivation to the optimal dynamic 2LLS and conclude the results here. Similar to $p_{t,i}^{(a)}$, let $p_{t,i}^{(b)}$ and $p_{t,i}^{(c)}$ $(0 \le p_{t,i}^{(b)} \le 1 - p_{t,i}^{(c)} \le 1)$ denote p_b and p_c at time t for an infected host in /16 subnet i. Assume that $N_i^{(16)}$ is the number of vulnerable hosts in /16 subnet i; $I_{t,i}^{(16)}$ is the number of infected hosts in /16 subnet i at time t; and $A_i^{(8)}$ is the set of /16 subnets that have the same first byte of the subnet address as /16 subnet i. Three items, $N_i^{(16)} - I_{t,i}^{(16)}$, $\frac{1}{2^8}\sum_{j\in A_i^{(8)}}(N_j^{(16)} - I_{t,j}^{(16)})$, and $\frac{1}{2^{16}}(N - I_t)$, are compared. The corresponding optimal 2LLS worm scanning strategy is summarized in Table I.

C. Experimental Results

In our experiments, we simulate the spread of a Witty worm, which has a vulnerable population $N = 55,909$ [18] and a scanning rate $s = 1,200$ per second [10]. The effect of disk damage on the Witty worm propagation is ignored. The worm is assumed to start spreading from one initially infected host (i.e., $I_0 = 1$).

We evaluate the propagation speed of optimal LS worms by two methods. The first method is the numerical analysis of the worm propagation models. Specifically, the spread of /l LS worms is simulated by Equations (5) and (8), while the propagation of 2LLS worms is implemented by Equations (5) and (13). The optimal /l LS uses Equations (5), (16), and (18). RS is regarded as a special case of the /l LS when $p_a = 0$ and an extreme example of the 2LLS when $p_b = p_c = 0$. The initially infected host is assumed to be located in the subnet that contains the smallest number of vulnerable hosts. Figure 2(a) compares the propagation speeds of RS, optimal /8 LS, and the /8 LS with $p_a = 0.75$. Figure 2(b) compares the spreading speeds of optimal 2LLS and the 2LLS with $p_b = 0.25$ and $p_c = 0.5$. It is shown that LS can spread much faster than RS, and the spreading speed of the currently used LS (i.e., 2LLS) can approach that of the optimal LS.

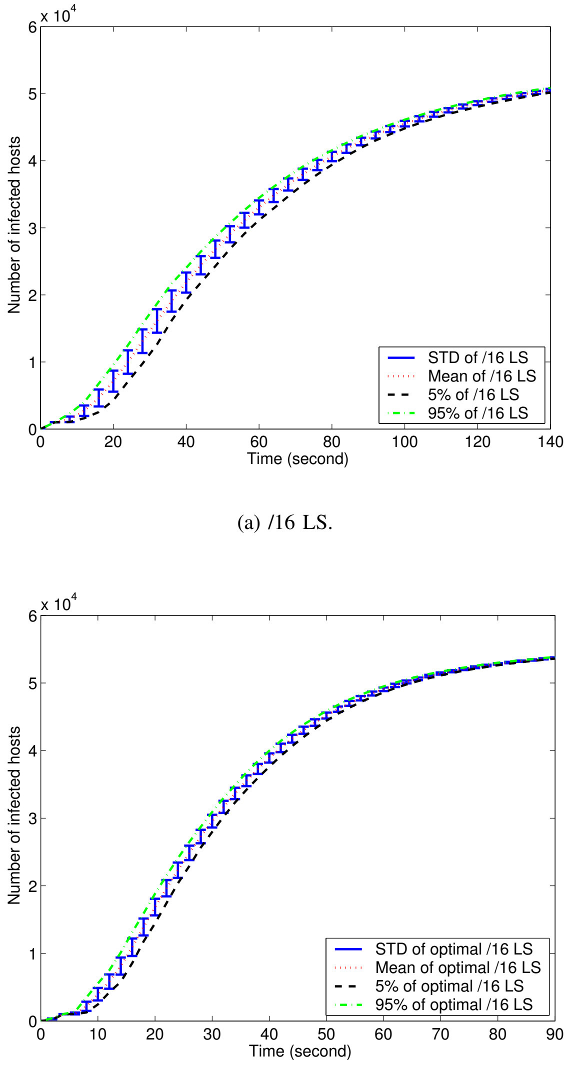
The second evaluation method uses a discrete event simulator to imitate the spread of LS worms. Our simulator implements each worm scan through a random number generator and simulates each scenario with 100 runs using different seeds. The initially infected host is located in the subnet that contains the largest number of vulnerable hosts. Figure 3(a) plots the mean and the variance of /16 LS worm propagation with $p_a = 0.75$. If a worm has a smaller variance, its spread is more predictable and stable. The "5%" (or "95%") propagation curve denotes that a worm spreads no slower (or faster) than this curve in 95 out of 100 simulation runs. The standard derivation (STD) error-bar reflects the variance of worm propagation among 100 simulation runs. It is observed that a /16 LS infected 50,318 (90%) vulnerable hosts in 138 seconds averagely. Figure 3(b) plots the simulation results of optimal /16 LS worm propagation. Such an optimal worm only



(a) /8 LS.

(b) 2LLS.

Fig. 2. Numerical analysis of (optimal) LS worm propagation.



(a) /16 LS.

(b) Optimal /16 LS.

Fig. 3. Simulations of /16 LS and optimal /16 LS worm propagation.

takes 65 seconds to infected 90% vulnerable hosts. Moreover, the optimal /16 LS has a smaller variance compared with the /16 LS.

V. Variants of Localized Scanning

In this section, we study three variants of LS that can be easily implemented and do not require information exchanges among infected hosts.

A. Decision-First Localized Scanning

The first variant is called *decision-first localized scanning* (DFLS). Instead of combining local scanning and global scanning, DFLS makes an infected host focus on scanning either locally or globally. For example, when a host is infected, it flips a coin and makes a decision:

- Scan only the local /l subnet with probability p_a,
- Scan globally with probability $1 - p_a$.

This scanning strategy is called /l DFLS, which is the counterpart of /l LS. Since in a /l subnet p_a percentage of infected hosts scan locally and $1 - p_a$ percentage of infected hosts use random scanning, Equations (5) and (8) still hold for /l DFLS.

We write a simulator to imitate the spread of DFLS worms and use the same setting as in Figure 3. Figure 4 plots the mean and the variance of /16 DFLS worm propagation with $p_a = 0.75$. It is observed that /16 DFLS spreads slower than /16 LS and on average takes 140 seconds to infect 40,000 vulnerable hosts. Moreover, /16 DFLS has a large variance as shown in the figure. This is because each infected host scans only either locally or globally. The hosts scanning globally have a slower speed to find a target. On the other hand, the hosts scanning locally waste scans after the local infected hosts become saturated. Thus, DFLS lacks a randomized algorithm

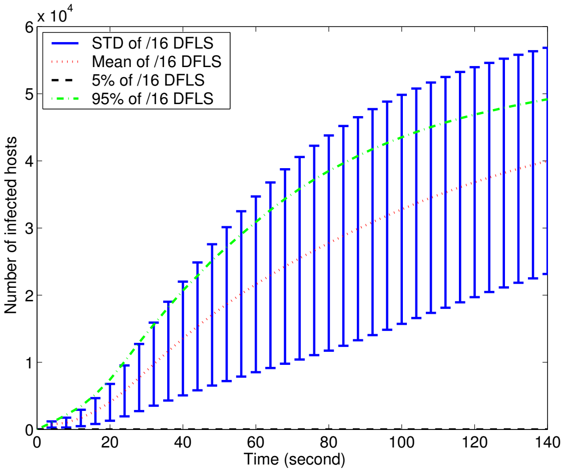


Fig. 4. Simulations of /16 DFLS worm propagation.

to search for targets both locally and globally and may not be a good candidate for worm attacks.

B. Feedback Localized Scanning and Ping-Pong Localized Scanning

The second variant is called *feedback localized scanning* (FLS), which is inspired by the optimal LS. The optimal strategy adapts the scanning methods, based on the local density of uninfected vulnerable hosts. In the similar way, we design a variant of LS, based on the feedback from the local probed host. For example, an infected host behaves as follows:

- First, initiates to scan the local /*l* subnet until probing a local host that has been already infected,
- Then, switches from scanning locally to scanning the global Internet.

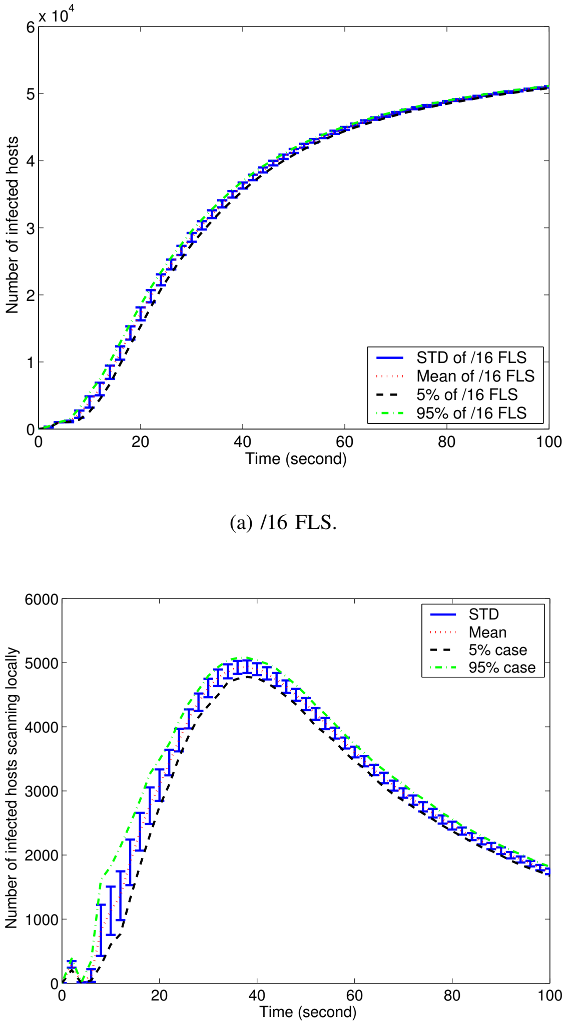
This scanning strategy is called /*l* FLS. The basic idea is that when the infected host probes a local host that has been already infected, it realizes that the infected hosts in the subnet probably have become saturated and had better switch to scanning globally.

We also write a simulator for FLS and show the results in Figure 5. Figure 5(a) plots the mean and the variance of /16 FLS worm propagation. It is observed that /16 FLS takes only 93 seconds to infect 90% vulnerable hosts and further approaches the spreading capacity of the optimal /16 LS. Moreover, /16 FLS has a small variance. Figure 5(b) further plots how the number of infected hosts that scans locally changes with time. It is shown that the number first increases with time and reaches the maximum after about 40 seconds and then decreases with time. This indicates that in the beginning many infected hosts focus on scanning locally and later switch to scanning globally. Therefore, FLS shows a better performance than the original LS and can be a potential tool for attackers.

FLS can further be extended to a "ping-pong" localized scanning (PPLS) method by adding the following algorithm:

- An infected host that uses random scanning will switch to scanning the local /*l* subnet when it probes a host that has been already infected.

Thus, an infected host switches between local scanning and global scanning, in an attempt to adapt to the underlying distribution of uninfected vulnerable hosts. Figure 6 plots the mean and the variance of /16 PPLS worm propagation. /16 PPLS further improves worm propagation at the late stage and only takes 81 seconds to infected 90% vulnerable hosts.



(a) /16 FLS.

(b) Number of infected hosts scanning locally.

Fig. 5. Simulations of /16 FLS worm propagation.

VI. Conclusions

In this paper, we attempt to understand the behaviors of localized-scanning (LS) worms through both analysis and simulation. We have shown analytically that an LS worm spreads slower than a random-scanning (RS) worm if the vulnerable-host distribution is uniform, or faster if highly uneven. Moreover, if the infected hosts are uniformly distributed,

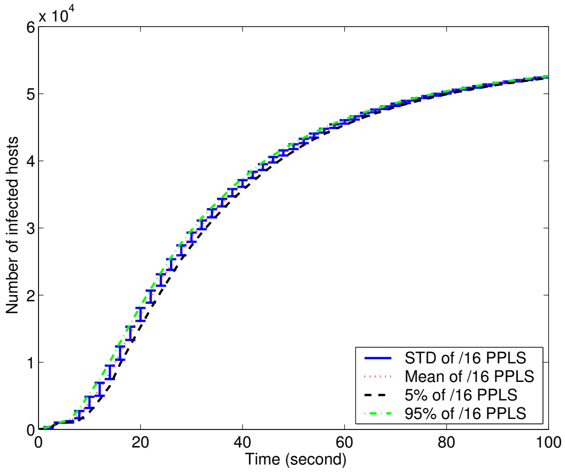


Fig. 6. Simulations of /16 PPLS worm propagation.

the LS method can increase the spreading speed by nearly a non-uniformity factor compared with the RS scheme.

We have designed the optimal dynamic LS worms. The spreading speed of such optimal LS can be approached by the currently used LS, showing that the existing LS is near-optimal. We have also constructed three variants of LS. While the decision-first localized scanning (DFLS) shows a poor performance empirically, the feedback localized scanning (FLS) and the ping-pong localized scanning (PPLS) demonstrate better performances than the original LS and can be good candidates for worm attacks. The key of FLS and PPLS is that a worm adapts its scanning strategies based on the feedback from the probed host.

As part of our ongoing work, we plan to develop effective detection/defense systems against LS worms.

ACKNOWLEDGEMENT

The authors would like to thank CAIDA for making the Witty dataset available. The authors would also like to thank the anonymous reviewers for their valuable comments. Support from NSF ECS 0300605 is gratefully acknowledged.

REFERENCES

[1] P. Barford, R. Nowak, R. Willett, and V. Yegneswaran, “Toward a model for sources of Internet background radiation,” in *Proc. of the Passive and Active Measurement Conference (PAM’06)*, Mar. 2006.

[2] Z. Chen, L. Gao, and K. Kwiat, “Modeling the spread of active worms,” in *Proc. of INFOCOM’03*, vol. 3, San Francisco, CA, Apr. 2003, pp. 1890-1900.

[3] Z. Chen and C. Ji, “A self-learning worm using importance scanning,” in *Proc. ACM/CCS Workshop on Rapid Malcode (WORM’05)*, Fairfax, VA, Nov. 2005, pp. 22-29.

[4] Z. Chen and C. Ji, “Optimal worm-scanning method using vulnerable-host distributions,” *to appear in the International Journal of Security and Networks: Special Issue on Computer and Network Security*, 2007.

[5] Z. Chen and C. Ji, “Measuring network-aware worm spreading ability,” in *Proc. of INFOCOM’07*, Anchorage, AK, May 2007.

[6] G. Gu, M. Sharif, X. Qin, D. Dagon, W. Lee, and G. Riley, “Worm detection, early warning and response based on local victim information,” in *Proc. 20th Ann. Computer Security Applications Conf. (ACSAC’04)*, Tucson, AZ, Dec. 2004.

[7] D. Moore, C. Shannon, and J. Brown, “Code-Red: a case study on the spread and victims of an Internet worm,” in *ACM SIGCOMM/USENIX Internet Measurement Workshop*, Marseille, France, Nov. 2002.

[8] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, “Inside the Slammer worm,” *IEEE Security and Privacy*, vol. 1, no. 4, July 2003, pp. 33-39.

[9] M. A. Rajab, F. Monrose, and A. Terzis, “On the effectiveness of distributed worm monitoring,” in *Proc. of the 14th USENIX Security Symposium (Security’05)*, Baltimore, MD, Aug. 2005.

[10] C. Shannon and D. Moore, “The spread of the Witty worm,” *IEEE Security and Privacy*, vol. 2, no. 4, Jul-Aug 2004, pp. 46-50.

[11] D. Song, R. Malan, and R. Stone, “A snapshot of global Internet worm activity,” *Technical Report*, 2001, http://www.arbor.net/downloads/research39/snapshot_worm_activity.pdf.

[12] S. Staniford, V. Paxson, and N. Weaver, “How to 0wn the Internet in your spare time,” in *Proc. of the 11th USENIX Security Symposium (Security’02)*, San Francisco, CA, Aug. 2002.

[13] E. W. Weisstein, “Chebyshev sum inequality,” *From MathWorld–A Wolfram Web Resource*, http://mathworld.wolfram.com/ChebyshevSumInequality.html.

[14] J. Wu, S. Vangala, L. Gao, and K. Kwiat, “An effective architecture and algorithm for detecting worms with various scan techniques,” in *Proc. 11th Ann. Network and Distributed System Security Symposium (NDSS’04)*, San Diego, CA, Feb. 2004.

[15] C. C. Zou, L. Gao, W. Gong, and D. Towsley, “Monitoring and early warning for Internet worms,” in *10th ACM Conference on Computer and Communication Security (CCS’03)*, Washington DC, Oct. 2003.

[16] C. C. Zou, D. Towsley, W. Gong, and S. Cai, “Routing worm: a fast, selective attack worm based on IP address information,” in *Proc. 19th ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation (PADS’05)*, Monterey, CA, June 2005.

[17] C. C. Zou, D. Towsley, and W. Gong, “On the performance of Internet worm scanning strategies,” *Elsevier Journal of Performance Evaluation*, vol. 63, no. 7, July 2006, pp. 700-723.

[18] The CAIDA Dataset on the Witty Worm - March 19-24, 2004, Colleen Shannon and David Moore, http://www.caida.org/passive/witty/. Support for the Witty Worm Dataset and the UCSD Network Telescope are provided by Cisco Systems, Limelight Networks, the US Department of Homeland Security, the National Science Foundation, and CAIDA, DARPA, Digital Envoy, and CAIDA Members.

[19] CERT Coordination Center, “‘Code Red II:’ another worm exploiting buffer overflow in IIS indexing service DLL,” CERT Incident Note IN-2001-09, http://www.cert.org/incident_notes/IN-2001-09.html.

[20] CERT Coordination Center, CERT Advisory CA-2001-26 Nimda Worm, http://www.cert.org/advisories/CA-2001-26.html.

[21] eEye Digital Security, “ANALYSIS: Blaster worm,” http://www.eeye.com/html/Research/Advisories/AL20030811.html.

[22] PanetMath.org, “Rearrangement inequality,” http://planetmath.org/encyclopedia/RearrangementInequality.html.

APPENDIX 1

Chebyshev Sum Inequality [13]

If $a_1 \geq a_2 \geq \cdots \geq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$, then

$$n \sum_{k=1}^{n} a_k b_k \geq \left(\sum_{k=1}^{n} a_k \right) \left(\sum_{k=1}^{n} b_k \right). \qquad (20)$$

The Chebyshev sum inequality follows from the rearrangement inequality [22].

APPENDIX 2

Rearrangement Inequality [22]

Let $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$ be real numbers. Then the sum $a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$ is maximized when the two sequences are ordered in the same way (i.e., $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$) and is minimized when the two sequences are ordered in the opposite way (i.e., $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$).